UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/028,164	10/25/2001	Thomas S. Messerges	CR00287M	3410

22917 7590 05/04/2005

MOTOROLA, INC.
1303 EAST ALGONQUIN ROAD
IL01/3RD
SCHAUMBURG, IL 60196

EXAMINER	
ABYANEH, ALI S	
ART UNIT	PAPER NUMBER
2133	

DATE MAILED: 05/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/028,164	**Applicant(s)** MESSERGES ET AL.	
	Examiner Ali S. Abyaneh	**Art Unit** 2133	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 October 2001*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-25* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 October 2001* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *1-21-03*.

4) □ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. Claims 1-25 are presented for examination.

Information Disclosure Statement PTO-1449

2. The Information Disclosure Statement submitted by applicant on 1/21/2003 has been considered. Please see attached PTO-1449.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless -
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-3, 9 and 15-18 are rejected under 35 U.S.C. 102(e) as being anticipated by William J. Bolosky et al. (US Publication NO. 2002/0194484)

Regarding Claim 1

Bolosky teaches a method of creating a signed content hash, comprising: dividing content into a plurality of chunks of content (paragraph [0072]); hashing each chunk of the plurality of chunks of content into a hash table; and signing the hash table ((paragraph

[0074] and [0168] –[170]) (examiner considers array 504 as applicant's hash table and manifest as applicant's signed hash table)).

Regarding Claim 2

Bolosky teaches all limitation of the claim as applied to claim 1 above and furthermore he teaches a method, wherein hashing each chunk of the plurality of chunks of content into the hash table comprises: calculating a chunk hash of each chunk of the plurality of chunks of content to provide a plurality of chunk hashes corresponding to the plurality of chunks of content; and storing the plurality of chunk hashes in the hash table (paragraph [0072] and [0074]).

Regarding Claim 3

Bolosky teaches all limitation of the claim as applied to claim 1 above and furthermore he teaches a method, wherein dividing the content into the plurality of chunks of content and hashing each chunk of the plurality of chunks of content into the hash table is repeated a plurality of times to create a corresponding plurality of hash tables (fig 5 and paragraph [0074]).

Regarding Claim 9

Bolosky teaches a method of authenticating a content hash, comprising: authenticating a hash table containing a plurality of chunk hashes corresponding to a plurality of chunks of content ((paragraph [0072], [0074] and [0148]-[0151]) (examiner considers array 504 as applicant's hash table)); dividing the content into a plurality of chunks of content (paragraph [0072]); and authenticating each chunk of the plurality of chunks of content (paragraph [0148]-[0151]).

Regarding Claim 15

Bolosky teaches all limitation of the claim as applied to claim 9 above and furthermore he teaches a method, wherein authenticating each chunk of the plurality of chunks of content comprises: calculating a recalculated chunk hash of the chunk of content to provide a recalculated chunk hash corresponding to the chunk of content; comparing the recalculated chunk hash to the chunk hash of the chunk stored in the hash table; and if the recalculated chunk hash matches the chunk hash of the chunk stored in the hash table, verifying the authenticity of the chunk (paragraph [0148]-[0151]).

Regarding Claims 16 and 17

Bolosky teaches all limitation of the claim as applied to claim 15 above and furthermore he teaches a method comprising: processing the chunk of content by having the recalculated chunk hash of the chunk of content calculated concurrently with calculating the recalculated chunk hash of the chunk and decrypting the chunk of content (paragraph [0156]); and rendering the chunk of content to the user (paragraph [0160]).

Regarding Claim 18

Bolosky teaches all limitation of the claim as applied to claim 9 above and furthermore he teaches a method, wherein dividing the content into the plurality of chunks of content and authenticating each chunk of the plurality of chunks of content is repeated a plurality of times to authenticate a corresponding plurality of hash tables (paragraph [0072]-[0075]).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) patent may not be obtained though the invention is not identically disclose or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 4-8, 10-14 and 19-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over William J. Bolosky et al. (US Publication NO. 2002/0194484) in view of Larry C. Puhl et al. (US Patent NO. 6,223,291).

Regarding Claims 4, 5 and 6

Bolosky teaches all limitation of the claim as applied to claim 1 above and furthermore teaches hash table in its entirety and comprises an overall hash of the hash table (paragraph [0159] and [0160]). Bolosky does not explicitly teach, wherein signing the hash table comprises: **creating a certificate of authenticity of the hash table; signing the certificate of authenticity of the hash table** and wherein **the certificate of authenticity of the hash table** comprises the hash table in its entirety and comprises an overall hash of the hash table. However, in an analogous art, Puhl teaches a method of **certificate of authenticity of the hash and signing the certificate of authenticity of the hash** (column 4, lines 30-35). Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Bolosky's method to include **certificate of authenticity of the hash table; signing the certificate of authenticity of the hash table** and **certificate of authenticity of the hash table** comprising the hash table in its entirety and an overall hash of the hash table. This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to verify the integrity of content by comparing a computed hash with the hash result in the certificate (column 4, lines 29-30).

Regarding Claim 7

Bolosky and Puhl teaches all limitation of the claim as applied to claim 6 above and furthermore Bolosky teaches a method, wherein creating the overall hash of the hash table comprises: hashing the plurality of chunk hashes stored in the hash table to create the overall hash of the hash table (paragraph [0109]-[0115]).

Regarding Claim 8

Bolosky and Puhl teach all limitation of the claim as applied to claim 4 above and furthermore Puhl teaches a method, wherein the certificate of authenticity of the hash table comprises additional information relating to the content and a set of rules governing the use of the content (column 3, lines 5-10).

Regarding Claims 10, 11 and 12

Bolosky teach all limitation of the claim as applied to claim 9 above and furthermore teaches a method of verifying a signature of a hash table and if the signature is verified authenticating the hash table and verifying the signature comprising the hash table in its entirety and if the signature of containing the hash table in its entirety is verified, verifying the authenticity of the hash table;.verifying a signature comprising an overall hash of the hash table; calculating a recalculated overall hash of the hash table; and if the recalculated overall hash of the hash table matches the overall hash of the hash table, verifying the authenticity of the hash table and if the signature is verified, verifying the authenticity of the hash table (paragraph [0148]-[0151]). Bolosky does not explicitly teach verifying a **certificate of authenticity** of the hash table; and if the **certificate of authenticity** of the hash table is verified, authenticating the hash table and verifying a signature of the **certificate of authenticity** comprising the hash table in its entirety and if the signature of the **certificate of authenticity** containing the hash table in its entirety is verified, verifying the authenticity of the hash table and verifying a signature of the **certificate of authenticity** comprising an overall hash of the hash table; calculating a recalculated overall hash of the hash table; and if the recalculated overall hash of the hash table matches the overall hash of the hash table and if the signature is verified,, verifying the authenticity of the hash table. However, in an analogous art, Puhl teaches a method of verifying a **certificate of authenticity** of the hash and verifying a signature of the **certificate of authenticity** (column 3, lines 60-67 and column4, lines 1-10). Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Bolosky's method to include verifying a **certificate of authenticity** of the hash table; and if the **certificate of authenticity** of the hash table is verified, authenticating the hash table and verifying a signature of the **certificate of authenticity** comprising the hash table in its entirety and if the signature of the **certificate of authenticity** containing the hash table in its entirety is verified, verifying the authenticity of the hash table and verifying a signature of the **certificate of authenticity** comprising an overall hash of the hash table; calculating a recalculated overall hash of the hash table; and if the recalculated overall hash of the hash table matches the overall hash of the hash table, verifying the authenticity of the hash table and if the signature is verified, verifying the authenticity of the hash table. This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to verify the integrity of the content by comparing computed hash with the hash result stored in the certificate (column 4, lines 26-31).

Regarding Claim 13

Bolosky and Puhl teach all limitation of the claim as applied to claim 12 above and furthermore Bolosky teaches a method, wherein calculating the recalculated overall hash of the hash table comprises: hashing the plurality of chunk hashes stored in the hash table to create the recalculated overall hash of the hash table (paragraph [0148]-[0151]).

Regarding Claim 14

Bolosky and Puhl teach all limitation of the claim as applied to claim 10 above and furthermore Puhl teaches a method, wherein verifying the certificate of authenticity of the hash further comprises: verifying additional information in the certificate of authenticity of the hash relating to the content and a set of rules governing the use of the content (column 3, lines 5-10).

Regarding Claim 19

Bolosky teaches a method of authenticating digital content, comprising: calculating an overall hash of a hash table; containing a plurality of chunk hashes corresponding to a plurality of chunks of content (([paragraph [0109]-[0115], [0072]-[0074]) (examiner considers array 504 as applicant's hash table)). Bolosky furthermore teaches comparing the hash value to the stored hash value for verification purpose (paragraph [0164]). Bolosky does not explicitly teach comparing the overall hash of the hash table to **a hash contained in a certificate**; and if the overall hash of the hash table matches the **hash of the certificate**, verifying the authenticity of the plurality of chunks of the content. However, in an analogous art, Puhl teaches a method wherein a computed hash is compared with a hash contained in the certificate (column 4, lines 30-5). Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Bolosky's method to include comparing the overall hash of the hash table to **a hash contained in a certificate**; and if the overall hash of the hash table matches the **hash of the certificate**, verifying the authenticity of the plurality of chunks of the content. This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to verify the integrity of the content by comparing computed hash with the hash result stored in the certificate (column 4, lines 26-31).

Regarding Claim 20

Bolosky and Puhl teach all limitation of the claim as applied to claim 19 above and furthermore Bolosky teaches a method, wherein further comprises for each chunk of the plurality of chunks of content: calculating a hash of the chunk to create a chunk hash of the chunk (paragraph [0074]); comparing the chunk hash to a stored chunk hash of the chunk stored in the hash table; and if the chunk hash matches the stored chunk hash, verifying the authenticity of the chunk (fig 9 and paragraph [0148]-[0151]).

Regarding Claim 21

Bolosky and Puhl teach all limitation of the claim as applied to claim 20 above and furthermore Bolosky teaches a method, wherein contemporaneously with calculating the hash of the chunk to create the chunk hash of the chunk, further comprising: decrypting the chunk to provide a chunk of decrypted content of the content package (paragraph [0156]); and rendering the chunk of decrypted content of the content package (paragraph [0160]).

Regarding Claim 22

Bolosky teaches a method of authenticating digital content, comprising: dividing content of a content package into a plurality of chunks of content (paragraph [0072]); calculating a chunk hash of each chunk of the plurality of chunks of content to provide a plurality of chunk hashes stored in a hash table corresponding to the plurality of chunks of content ((paragraph [0072] and [0074]) (examiner considers array 504 as applicant's hash table)); hashing the plurality of chunk hashes of the hash table to create an overall hash of the content of the content package (paragraph [109]-[0115]); determining whether a recalculated overall hash of the hash table matches the overall hash of the hash table; if the recalculated hash of the hash table matches the overall hash of the hash table, verifying the authenticity of each chunk of the plurality of chunks of the content (fig 9 and paragraph [0148]-[0151]). Bolosky does not explicitly teach placing the overall hash into a **certificate.** However, in an analogous art, Puhl teaches a method wherein a hash result is placed into a **certificate** (column 4, lines 29-30). Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Bolosky's method to include placing the overall hash into a **certificate**. This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to verify the integrity of the content by comparing computed hash with the hash result stored in the certificate (column 4, lines 28-30).

Regarding Claim 23

Bolosky and Puhl teach all limitation of the claim as applied to claim 22 above and furthermore Bolosky teaches a method, wherein determining whether the recalculated overall hash of the hash table matches the overall hash of the hash table comprises: recalculating the overall hash of the hash table to create the recalculated overall hash; comparing the recalculated overall hash to the overall hash; and if the recalculated overall hash matches the overall hash and a signature on the certificate is valid, verifying authenticity of the hash table (paragraph [0148]-[0151]).

Regarding Claim 24

Bolosky and Puhl teach all limitation of the claim as applied to claim 22 above and furthermore Bolosky teaches a method, wherein verifying the authenticity of each chunk of the plurality of chunks comprises for each chunk: recalculating a hash of the chunk to create a recalculated chunk hash of the chunk; comparing the recalculated chunk hash to the chunk hash of the chunk; and if the recalculated chunk hash matches the chunk hash of the chunk, verifying the authenticity of the chunk (paragraph [0148]-[0151]).

Regarding Claim 25

Bolosky and Puhl teach all limitation of the claim as applied to claim 24 above and furthermore Bolosky teaches a method, wherein contemporaneously with recalculating the hash of the chunk to create the recalculated chunk hash of the chunk, further comprising: decrypting the chunk to provide a chunk of decrypted content of the content package (paragraph [0156]); and rendering the chunk of decrypted content of the content package (paragraph [0160]).

References Cited, Not Used

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

1. U.S. Publication No. 2001/0032310

This reference relates to public key cryptosystems, and more particularly, to a public key validation service for validating a public key.

2. U.S.Patent No. 6,847,995

This reference relates to distributing project workloads among a distributed device and more particularly to techniques and related methods for managing, facilitating and implementing distributed processing in a network environment.

Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ali Abyaneh whose telephone number is (571) 272-7961. The examiner can normally be reached on Monday-Friday from (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert Decady can be reached on (571)272-3819. The fax phone numbers for the organization where this application or proceeding is assigned as (703) 872-9306. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ali Abyaneh A.A
Patent Examiner
Art Unit 2133
04/25/05

GUY LAMARRE
PRIMARY EXAMINEP